REMARKS

The Examiner has objected to the specification. Such objection is deemed moot in view of the clarifications made hereinabove.

The Examiner has rejected Claims 1-3, 6-12, 15-21, 24-27 under 35 U.S.C. 102(e) as being anticipated by Schertz et al. (U.S. Publication No. 2003/0084322 A1). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on the following excerpts from the Schertz reference to make a prior art showing of applicant's claimed "detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger..." (see this or similar, but not necessarily identical language in each of the independent claims).

> "[0018] The operating system-integrated intrusion detection system may be one that employs network-based, host-based and inline intrusion protection as shown in FIG. 2. Each intrusion detection system component may be operating system-integrated or not. Network-based intrusion protection systems are generally deployed at or near the entry point of a network, such as a firewall. **Network-based intrusion protection systems analyze data inbound from the Internet and collects network packets to compare against a database of various known attack signatures or bit patterns.** An alert may be generated and transmitted to a management system that may perform a corrective action such as closing communications on a port of the firewall to prevent delivery of the identified packets into the network. Network-based intrusion protection systems generally provide real-time, or near real-time, detection of attacks. **Thus, protective actions may be executed before damage is made to the targeted system.** Furthermore, network-based intrusion protection systems are effective when implemented on slow communication links such as ISDN or T1 Internet connections. Moreover, network-based intrusion protection systems are easy to deploy. Typically, network-based intrusion protection systems are placed at or near the boundary of the network being protected." (Paragraph 0018 - emphasis added)

"[0021] Referring to FIG. 2, one or more networks 100 may interface with the Internet 50 via a router 40 or another suitable device. In network 100, for example, two Ethernet networks 55 and 56 are coupled to the Internet 50 via router 40. Ethernet network 55 includes a firewall/proxy server 60 coupled to a web-content server 61 and a file transport protocol content server 62. Ethernet network 56 includes a domain name server (DNS) 70 coupled to a mail server 71, a database sever 72, and a file server 73. **Network-based intrusion protection systems** deployed on dedicated appliances 80 and 81 are disposed on two sides of firewall/proxy server 60 to facilitate monitoring of attempted attacks against one or more nodes of network 100 and to facilitate recording successful attacks that successfully penetrate firewall/proxy server 60. Network intrusion protection devices 80 and 81 may respectively include (or alternatively be connected to) databases 80a and 81a containing known attack signatures. Accordingly, network intrusion protection device 80 may monitor all packets inbound from Internet 50. Similarly, network intrusion protection device 81 monitors and compares all packets that passed by firewall/proxy server 60 for delivery to Ethernet network 56." (Paragraph 0021 – emphasis added)

"[0023] Preferably, network intrusion protection devices 80 and 81 are dedicated entities for monitoring network traffic on associated links of network 100. To facilitate intrusion protection in high speed networks, network intrusion protection devices 80 and 81 preferably include a large capture RAM (random access memory) for capturing packets as the arrive on respective Ethernet networks 55 and 56. Additionally, it is preferable that network intrusion protection devices 80 and 81 respectively include hardware-based filters for filtering high-speed network traffic. Filters may be alternatively implemented in software at a loss of speed and corresponding potential losses in protective abilities provided thereby to network 100. Moreover, network intrusion protection devices 80 and 81 may be configured, for example by demand of IPS management node 85, to monitor one or more specific devices rather than all devices on a network. For example, network intrusion protection device 80 may be instructed to monitor only network data traffic addressed to web server 61. Hybrid host-based and inline-based intrusion protection system technologies may be implemented on all other servers on Ethernet networks 55 and 56 that may be targeted in a distributed system attack. A distributed intrusion protection system such as the one described above may be integrated with any number of platforms, such as UNIX, WINDOWS NT, WINDOWS, LINUX, etc." (Paragraph 0023 – emphasis added)

The above excerpts from Schertz teach a method of performing network-based intrusion detection on packets inbound from the internet via a firewall or proxy server destined for a device or multiple devices on the network. These packets are compared to a database containing known attack signatures and bit patterns. In sharp contrast, applicant claims "detecting code for detecting from said plurality of log data messages

received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger..." (emphasis added), in the context claimed.

Also, the Examiner has rejected Claims 1, 10, and 19 as being unpatentable over Hypponen et al (U.S. Publication No. 2003/0191957 A1). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has further relied on the following excerpts from the Hypponen reference to make a prior art showing of applicant's claimed "detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger..." (see this or similar, but not necessarily identical language in each of the independent claims). Applicant has carefully considered the entire Hypponen reference and has included paragraphs 0029 and 0034 below for additional context on Figure 1.

> "[0035] Each of the protected systems 4 has stored in its memory a so-called "agent" program which is run by the system, in the background to the normal tasks performed by the systems. The agent's function is to intercept data which is being transferred through the system 4 on which the agent is running. The intercepted data is scanned on-the-fly by the agent to determine whether or not the data has a form which may contain a virus. Thus, the agent may identify data files having the .doc, .dot, .exe, etc, extensions. Considering for example the firewall 4a, this will intercept and scan data being transferred from the Internet 5 to the network 3, and possibly data traveling in the opposite direction. Similarly, the mail server 4b and proxy server 4c will intercept and scan mail and WWW data respectively, whilst the database server 4d scans data being transferred to and from the data storage facility 6. Of course the network may be arranged such that the unnecessary duplication of tasks is avoided, e.g. the mail server 4b does not scan data received from the firewall 4a but only scans internally transferred mail." (Paragraph 0035 - emphasis added)
>
> "[0036] Data which is not of a suspect type is passed over by the agent and is routed by the system to its intended user 2.

However, any data which is identified by the agent as being suspect, is re-routed over the network 1, from the protected system in question, to the virus scanning server 7. Upon receipt of the suspect data, the server 7 scans the data for viruses. This scanning may be performed by one of a number of known scanning systems including F-PROT TM and F-SECURE TM available from DataFellows (Helsinki, Finland)." (Paragraph 0036 - emphasis added)

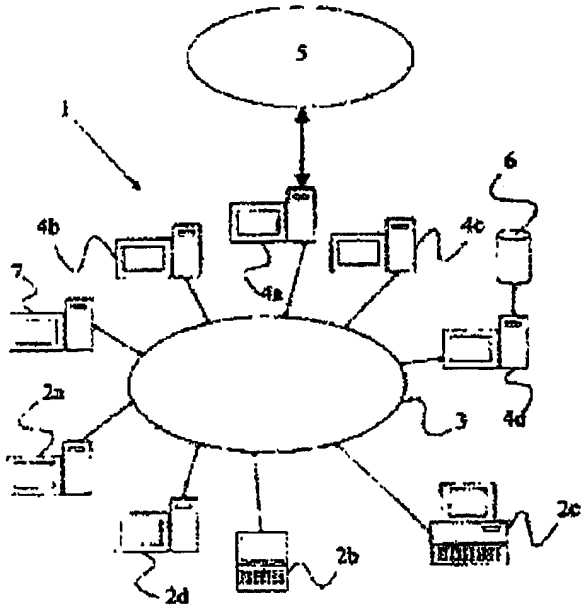

Figure 1

"[0029] FIG. 1 shows schematically a data network having a central virus scanning server; and" (Paragraph 0029 - emphasis added)

"[0034] An additional server 7 provides virus scanning functionality as will be described below. This virus scanning server 7 is coupled to the network 1 and in use communicates with the protected systems 4 and the administrator's work station 2a. The server 7 is able to communicate with the protected systems 4 and workstation 2a using for example proprietary and standardised protocols carried over the TCP/IP network 3." (Paragraph 0034 emphasis added)

The excerpts from Hypponen teach virus scanning data flowing through protected systems. These protected systems communicate with a central virus scanning server that determines if the intercepted data contains a virus. The virus scanning of intercepted data is performed on only those systems deemed as protected systems. There is no disclosure,

however, of the use of "a pattern and a network-wide threshold of malware detection" (emphasis added), as claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the above reference, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, as follows:

> "the network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers" (see this or similar, but not necessarily identical language in each of the independent claims).

Thus, applicant has further elaborated on the claimed network-wide threshold to further distinguish the prior art of record. Specifically, it is clarified that the network-wide threshold is applied to a sum of detections, where the detections are each particularly associated with a different one of the network connected computers. A notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 6 et al., the Examiner has relied on the following excerpts from Schertz to make a prior art showing of applicant's claimed technique "wherein said at least one predetermined anti-malware action includes isolating at least one of said network connected computers from other parts of said computer network."

> "Furthermore, OS-integrated anti-virus system 16 would prevent storage of the virus payload (154), and further transmission of the virus payload to other host processors (156). Finally, execution of the virus payload is also monitored and avoided by OS-integrated anti-virus system 16 (158). These functional blocks may represent either hardware modules or software processes that serve the functionality described." (Paragraph 0031, lines 17-24 - emphasis added)

> "Additionally, an attack may be prevented because an inline intrusion protection system may discard data identified as associated with an attack rather than pass the data to the application layer for processing." (Paragraph 0020, lines 14-17 - emphasis added)

Applicant respectfully asserts that the above excerpts from Schertz, as relied upon by the Examiner, teach preventing the storage of a virus payload by the anti-virus system and transmission to other host processors. The second excerpt teaches an inline intrusion protection system that may discard data identified as being associated with an attack. The Schertz excerpts, however, fail to even suggest a technique of "... isolating at least one of said network connected computers from other parts of said computer network" (emphasis added), as claimed.

Further, with respect to Claim 7 et al., the Examiner has relied on the following excerpts from Schertz to make a prior art showing of applicant's claimed technique "wherein said managing computer stores said plurality of log data messages within a database." To provide additional context on Figure 2 and, in particular, items 80A and 81A, an excerpt from paragraph 0021 is referenced below.

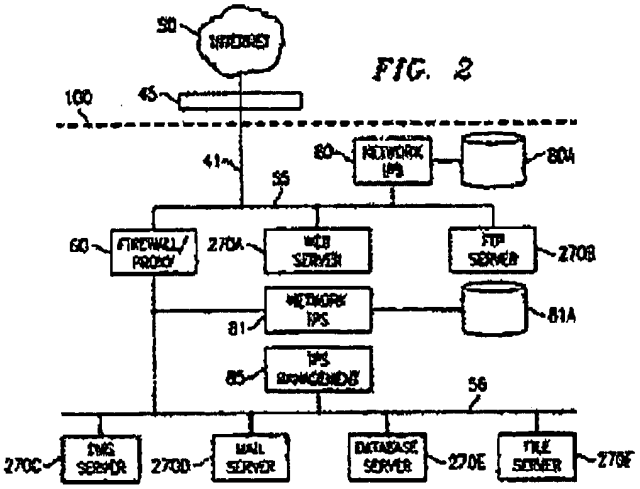

FIG. 2

(Figure 2, items 80A and 81A)

"Network intrusion protection devices 80 and 81 may respectively include (or alternatively be connected to) databases 80a and 81a containing known attack signatures." (Paragraph 0021, lines 15-18 - emphasis added)

Applicant respectfully asserts that items 80A, and 81A in Figure 2 relied upon by the Examiner disclose storing known attack signatures in databases for the network intrusion protection devices. However, applicant claims a technique "wherein said managing computer stores said plurality of log data messages within a database" (emphasis added), in the claimed context. Since the excerpts fail to disclose storing log messages in a database, Schertz clearly fails to disclose applicant's claimed technique.

In addition, with respect to Claim 4 et al., the Examiner has rejected the same under 35 U.S.C 103(a) as being unpatentable over Schertz et al (U.S. Publication No. 2003/0084322 A1) in view of Schnurer et al (U.S. Patent No. 5,842,002). Specifically, the Examiner has relied on the following excerpt from Schnurer to make a prior art showing of applicant's claimed technique "wherein said at least one predetermined anti-malware action includes forcing an update of malware definition data being used by one or more of said plurality of network connected computers."

"Yet another object of the present invention is to provide a virus detection system able to detect as of yet unknown viruses thereby obviating the need for software updates to keep the detection device current." (Col. 5, lines 16-19 - emphasis added)

Applicant respectfully asserts that the excerpt from Schnurer teaches a system where software updates that keep the detection device current are unnecessary. In stark contrast, applicant claims a technique "wherein said at least one predetermined anti-malware action includes forcing an update of malware definition data being used by one or more of said plurality of network connected computers" (emphasis added), in the context claimed. Hence, Schnurer cleary fails to disclose applicant's claimed technique.

Furthermore, with respect to Claim 5 et al., the Examiner has rejected the same as being unpatentable over Schertz et al. (U.S. Publication No. 2003/0084322 A1) in view of Chen et al (U.S. Patent No. 5,832,208). Specifically, the Examiner has relied on the following excerpts from Chen to make a prior art showing of applicant's claimed technique "wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one of said malware scanners such that said at least one of said malware scanners performs more thorough malware scanning." To provide additional context to item 260 in Figure 3, applicant has included an additional excerpt from Chen below.

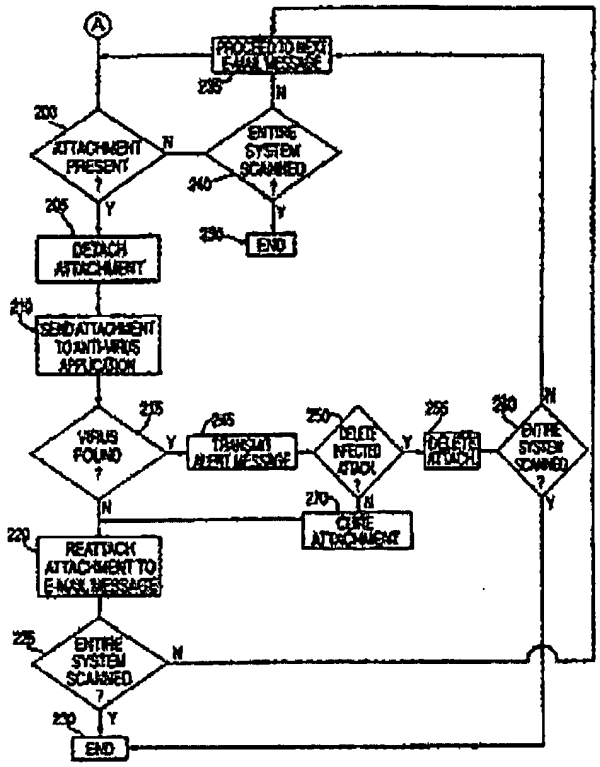

FIG. 3

(Figure 3, item 260)

"After step 255, the agent 110 determines if the entire mail system 140 has been scanned (step 260). If so, then the process has reached an end (step 230). If the entire mail system 140 has not been scanned, then the agent 110 proceeds to the next e-mail message (step 235)." (Col. 8, lines 1-5 - emphasis added)

Applicant respectfully asserts that the above figure from Chen relied upon by the Examiner teaches scanning an entire mail system, one email message at a time. After processing and handling a virus found in a single email message, the system then checks to see if the entire mail system was scanned before branching to an end block. Furthermore, if the email attachment does not contain a virus, the system will still check to see if the entire mail system was scanned. Hence, there is no increase in scanning thoroughness after the virus is detected. This technique of checking all email messages does not even suggest applicant's claimed technique "wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least

one of said malware scanners such that said at least one of said malware scanners performs more thorough malware scanning" (emphasis added), as claimed. Since the Chen excerpts above do not disclose "perform[ing] more thorough malware scanning" (emphasis added), as claimed, such excerpts fail to disclose applicant's claimed technique.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 28-29 below, which are added for full consideration:

"wherein predefined network-wide thresholds and patterns are provided as templates" (see Claim 28); and

"wherein predefined network-wide thresholds and patterns are customized to particular circumstances" (see Claim 29).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P461).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100